

Convolutional Codes Derived From Group Character Codes

Giuliano G. La Guardia *

December 20, 2012

Abstract

New families of unit memory as well as multi-memory convolutional codes are constructed algebraically in this paper. These convolutional codes are derived from the class of group character codes. The proposed codes have basic generator matrices, consequently, they are non catastrophic. Additionally, the new code parameters are better than the ones available in the literature.

1 Introduction

Constructions of (classical) convolutional codes and their corresponding properties have been presented in the literature [1, 3–8, 12, 15–20]. In [3], the author constructed an algebraic structure for convolutional codes. Addressing the construction of maximum-distance-separable (MDS) convolutional codes (in the sense that the codes attain the generalized Singleton bound introduced in [18, Theorem 2.2]), there exist interesting papers in the literature [5, 18, 20]. Concerning the optimality with respect to other bounds we have [16, 17], and in [4], Strongly MDS convolutional codes were constructed. In [1, 8, 12, 19], the authors presented constructions of convolutional BCH codes. In [6], doubly-cyclic convolutional codes were constructed and in [7], the authors described cyclic convolutional codes by means of the matrix ring.

In this paper we construct families of unit memory as well as multi-memory convolutional codes, although it is well known that unit memory codes have large free distance when compared to multi-memory codes of same rate (see [13]). Our constructions are performed algebraically and not by computation search. Consequently, we do not restrict ourselves in constructing only few specific codes. To do so we apply the famous method proposed by Piret [15] and recently generalized by Aly *et al.* [1, Theorem 3], which consists in the construction of convolutional codes derived from block codes. The block codes utilized in our construction is the subclass of 2-group character codes introduced

*Giuliano Gadioli La Guardia is with Department of Mathematics and Statistics, State University of Ponta Grossa (UEPG), 84030-900, Ponta Grossa, PR, Brazil.

by Ding *et al.* [2] as well as its generalization to n -group, ($n \geq 2$) character codes [14].

The new families of convolutional codes consist of codes whose parameters are given by

- $(2^m, 2^m - s_m(u), s_m(u) - s_m(r); 1, d_f \geq 2^{r+1})_q,$

- $(2^m, s_m(u), s_m(u) - s_m(r); \mu, d_f^\perp \geq 2^{m-u} + 1)_q,$

where q is a power of an odd prime, $m \geq 3$ is an integer, r and u are positive integers satisfying $r < u < m$ and $\sum_{i=u+1}^m \binom{m}{i} > \sum_{i=r+1}^u \binom{m}{i}$, $\mu \geq 1$ is an integer and $s_m(v) = \sum_{i=0}^v \binom{m}{i}$;

- $(2^m, 2^m - s_m(u), \delta; 2, d_f \geq 2^{r+1})_q,$

where q is a power of an odd prime, $m \geq 4$ is an integer, $s_m(u)$ is given above, $\delta = \sum_{i=r+1}^v \binom{m}{i}$, and r, u, v are positive integers such that the inequalities $r < v < u < m$, $\sum_{i=u+1}^m \binom{m}{i} \geq \sum_{i=r+1}^v \binom{m}{i} \geq \sum_{i=v+1}^u \binom{m}{i}$ hold;

- $(l^m, l^m - S_m(u), S_m(u) - S_m(r); 1, d_f \geq (b+2)l^a)_q,$

where $m \geq 3$, $l \geq 3$ are integers, q is a prime power such that $l|(q-1)$, r and u are positive integers satisfying the inequalities $r < u < m(l-1)$ and $\sum_{i=u+1}^m \binom{m}{i}_l \geq \sum_{i=r+1}^u \binom{m}{i}_l$, a and b are integers such that $r = a(l-1) + b$, $0 \leq b \leq l-2$ and $S_m(v) = \sum_{i=0}^v \sum_{k=0}^m (-1)^k \binom{m}{k} \binom{m-1+i-kl}{m-1}$.

The paper is organized as follows. In Section 2, we recall basic concepts and results concerning the class of character codes. Section 3 deals with basic definitions and known results on convolutional codes. In Section 4, the contributions of the work are presented, that is, the constructions of new families of convolutional codes derived from character codes. In Section 5, we compare the new code parameters with the ones available in the literature, and finally, in Section 6, a summary of the paper is described.

2 Character Codes

Throughout this paper, p denotes a prime number, q is a prime power and \mathbb{F}_q is a finite field with q elements. As usual, the parameters of a linear code are given by $[n, k, d]_q$, and the notation $\text{wt}_H(x)$ means the Hamming weight of a vector $\mathbf{x} \in \mathbb{F}_q^n$.

The class of group character codes were introduced by Ding *et al.* [2]. These codes are defined by using characters of groups; they are linear, defined over \mathbb{F}_q and are similar (with respect to the parameters) to binary Reed-Muller codes.

In order to define such class of codes, let us consider an abelian group $(G, +)$ of order n and exponent N and let \mathbb{F}_q be a finite field such that $\gcd(n, q) = 1$ and $N|(q-1)$. Assume also that (\mathbb{F}_q^*, \cdot) is the multiplicative group of nonzero elements of \mathbb{F}_q . Then a character γ from $(G, +)$ to (\mathbb{F}_q^*, \cdot) is a homomorphism of groups (in which, from our assumptions, the operation among characters is the multiplication). We denote the group of characters by (Γ, \cdot) . Since in this case $(G, +)$ is isomorphic to (Γ, \cdot) , then there exists a bijection $g \in G \rightarrow \gamma_g \in \Gamma$ and we can denote $\Gamma = \{\gamma_0, \dots, \gamma_{n-1}\}$ (γ_0 is the trivial character). For every $X \subset G$, the *group character code* C_X is a linear code over \mathbb{F}_q defined

by $C_X = \left\{ (c_0, \dots, c_{n-1}) \in \mathbb{F}_q^n \mid \sum_{i=0}^{n-1} c_i \gamma_i(x) = 0, \forall x \in X \right\}$ and has parameters $[n, k]_q$, where $n = |G|$ and $k = n - |X|$ (see [2]). If $X = \{x_0, \dots, x_{s-1}\} \subset G$ then a generator matrix for C_X is given by $G_X = [\gamma_{j-1}(-x_{s-1+i})]_{1 \leq i \leq n-s, 1 \leq j \leq n}$; a parity check matrix for C_X is given by $H_X = [\gamma_{j-1}(x_{i-1})]_{1 \leq i \leq s, 1 \leq j \leq n}$.

A particular case is when it is considered the commutative group $(\mathbb{Z}_2^m, +)$, with $m \geq 1$, and a finite field \mathbb{F}_q of odd characteristic. The characters of \mathbb{Z}_2^m are given by $\gamma_{\mathbf{x}}(\mathbf{y}) = (-1)^{\mathbf{x} \cdot \mathbf{y}}$, where $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^m$. Then one defines the character code $C_q(r, m) = C_{X_r}$, where $X_r = \{\mathbf{x} \in \mathbb{Z}_2^m \mid \text{wt}_H(\mathbf{x}) > r\}$, with parameters $[2^m, s_m(r), 2^{m-r}]_q$ (see [2, Theorem 6]), where $s_m(r) = \sum_{i=0}^r \binom{m}{i}$. Its (Euclidean)

dual code $[C_q(r, m)]^\perp$ is equivalent to $C_q(m-r-1, m)$ (see [2, Theorem 8]).

In 2004, Ling [14] generalized such class of codes by considering the group $(\mathbb{Z}_l^m, +)$, where $m \geq 1$ and $l \geq 2$ are integers and \mathbb{F}_q is a finite field that contains a l th root of unity, that is, $l|(q-1)$. Let $\mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}_l^m$ and assume that $\|\mathbf{x}\| = x_1 + \dots + x_m$, where the sum is considered as a rational integer. Analogously to X_r , one can define the set $X(r, m; l) = \{\mathbf{x} \in \mathbb{Z}_l^m : \|\mathbf{x}\| > r\}$, generating the linear q -ary group character code $C_q(r, m; l) = \left\{ (c_0, \dots, c_{l^m-1}) \in \mathbb{F}_q^{l^m} \mid \sum_{i=0}^{l^m-1} c_i \gamma_i(\mathbf{x}) = 0, \forall \mathbf{x} \in X(r, m; l) \right\}$, where $\gamma_0, \dots, \gamma_{l^m-1}$, are all the characters from \mathbb{Z}_l^m to \mathbb{F}_q^* . To be more precise, if ξ is a fixed l th root of unity, then the characters $\gamma_i : \mathbb{Z}_l^m \rightarrow \mathbb{F}_q^*$, $i = 0, \dots, l^m-1$, are given by $\gamma_i((x_1, \dots, x_m)) = \xi^{x_1 i_1 + \dots + x_m i_m}$, where the coefficients i_k , $k = 1, \dots, m$, are the coefficients of the (unique) l -adic expansion of i . The code $C_q(r, m; l)$ has parameters $[l^m, S_m(r), (l-b)l^{m-1-a}]_q$, where $0 \leq r < m(l-1)$ is writing as $r =$

$$a(l-1)+b, 0 \leq b \leq l-2, \text{ and } S_m(r) = \sum_{i=0}^r \sum_{k=0}^m (-1)^k \binom{m}{k} \binom{m-1+i-kl}{m-1}.$$

Furthermore, its (Euclidean) dual code $[C_q(r, m; l)]^\perp$ is monomial equivalent to $C_q(m(l-1) - 1 - r, m; l)$ (see [14]).

3 Convolutional Codes

In this section we present a brief review of convolutional codes. For more details we refer the reader to [9, 10, 15].

Recall that a polynomial encoder matrix $G(D) \in \mathbb{F}_q[D]^{k \times n}$ is called *basic* if $G(D)$ has a polynomial right inverse. A basic generator matrix of a convolutional code C is called *reduced* (or minimal [7, 9, 20]) if the overall constraint length

$\delta = \sum_{i=1}^k \delta_i$ has the smallest value among all basic generator matrices of C ; in this case the overall constraint length δ is called the *degree* of the code. The

weight of an element $\mathbf{v}(D) \in \mathbb{F}_q[D]^n$ is defined as $\text{wt}(\mathbf{v}(D)) = \sum_{i=1}^n \text{wt}(v_i(D))$,

where $\text{wt}(v_i(D))$ is the number of nonzero coefficients of $v_i(D)$.

Definition 3.1 [10] *A rate k/n convolutional code C with parameters $(n, k, \delta; \mu, d_f)_q$ is a submodule of $\mathbb{F}_q[D]^n$ generated by a reduced basic matrix $G(D) = (g_{ij}) \in \mathbb{F}_q[D]^{k \times n}$, that is, $C = \{\mathbf{u}(D)G(D) \mid \mathbf{u}(D) \in \mathbb{F}_q[D]^k\}$, where n is the length, k is the dimension, $\delta = \sum_{i=1}^k \delta_i$ is the degree, where $\delta_i = \max_{1 \leq j \leq n} \{\deg g_{ij}\}$,*

$\mu = \max_{1 \leq i \leq k} \{\delta_i\}$ is the memory and $d_f = \text{wt}(C) = \min\{\text{wt}(\mathbf{v}(D)) \mid \mathbf{v}(D) \in C, \mathbf{v}(D) \neq 0\}$ is the free distance of the code.

If $\mathbb{F}_q((D))$ is the field of Laurent series we define the weight of $\mathbf{u}(D)$ as $\text{wt}(\mathbf{u}(D)) = \sum_{\mathbb{Z}} \text{wt}(u_i)$. A generator matrix $G(D)$ is called *catastrophic* if there exists a $\mathbf{u}(D)^k \in \mathbb{F}_q((D))^k$ of infinite Hamming weight such that $\mathbf{u}(D)^k G(D)$ has finite Hamming weight. The convolutional codes constructed in this paper have basic generator matrices; consequently, they are non catastrophic.

We define the Euclidean inner product of two n -tuples $\mathbf{u}(D) = \sum_i \mathbf{u}_i D^i$ and $\mathbf{v}(D) = \sum_j \mathbf{v}_j D^j$ in $\mathbb{F}_q[D]^n$ as $\langle \mathbf{u}(D) \mid \mathbf{v}(D) \rangle = \sum_i \mathbf{u}_i \cdot \mathbf{v}_i$. If C is a convolutional code then its (Euclidean) dual is given by $C^\perp = \{\mathbf{u}(D) \in \mathbb{F}_q[D]^n \mid \langle \mathbf{u}(D) \mid \mathbf{v}(D) \rangle = 0 \text{ for all } \mathbf{v}(D) \in C\}$.

3.1 Convolutional Codes Derived From Block Codes

Let $[n, k, d]_q$ be a block code whose parity check matrix H is partitioned into $\mu + 1$ disjoint submatrices H_i such that $H = [H_0 \ H_1 \ \cdots \ H_\mu]^T$, where each H_i has n columns, obtaining the polynomial matrix

$$G(D) = \tilde{H}_0 + \tilde{H}_1 D + \tilde{H}_2 D^2 + \cdots + \tilde{H}_\mu D^\mu. \quad (1)$$

The matrix $G(D)$ generates a convolutional code V with κ rows, where κ is the maximal number of rows among the matrices H_i ; the matrices \tilde{H}_i , where $0 \leq i \leq \mu$, are derived from the respective H_i by adding zero-rows at the bottom in such a way that the matrix \tilde{H}_i has κ rows in total.

Theorem 3.1 [1, Theorem 3] Suppose that $C \subseteq \mathbb{F}_q^n$ is an $[n, k, d]_q$ code with parity check matrix $H \in \mathbb{F}_q^{(n-k) \times n}$ partitioned into submatrices H_0, H_1, \dots, H_μ as above such that $\kappa = \text{rk} H_0$ and $\text{rk} H_i \leq \kappa$ for $1 \leq i \leq \mu$. Then the matrix $G(D)$ is a reduced basic generator matrix. Moreover, if d_f and d_f^\perp denote the free distances of V and V^\perp , respectively, d_i denote the minimum distance of the code $C_i = \{\mathbf{v} \in \mathbb{F}_q^n \mid \mathbf{v} \tilde{H}_i^t = 0\}$ and d^\perp is the minimum distance of C^\perp , then one has $\min\{d_0 + d_\mu, d\} \leq d_f^\perp \leq d$ and $d_f \geq d^\perp$.

4 The New Codes

Constructions of convolutional codes have been appeared in the literature [4–8, 15, 18, 20]. It is not simple to derive families of such codes by means of algebraic approaches. In other words, most of the convolutional codes available in the literature are constructed case by case.

Motivated by the construction of new convolutional codes by means of algebraic method, we propose the construction of new convolutional codes derived from character codes. We reinforce that the convolutional codes constructed in this paper have basic generator matrices, so they are non catastrophic. Our first main result is given in the following:

Theorem 4.1 Let \mathbb{F}_q be a finite field of odd characteristic and consider the commutative group $G = (\mathbb{Z}_2^m, +)$ where $m \geq 3$ is an integer. Assume that r and u are positive integers such that the inequalities $r < u < m$ and $\sum_{i=u+1}^m \binom{m}{i} \geq \sum_{i=r+1}^u \binom{m}{i}$ hold. Then there exist unit memory convolutional codes with parameters $(2^m, 2^m - s_m(u), s_m(u) - s_m(r); 1, d_f \geq 2^{r+1})_q$, where $s_m(u)$ and $s_m(r)$ are given in Section 2.

Proof: Assume that $n = 2^m$, $r \geq 1$ is an integer, $X_r = \{\mathbf{x} \in \mathbb{Z}_2^m \mid \text{wt}_H(\mathbf{x}) > r\}$ and let $C_q(r, m) = C_{X_r}$ be the character code with parameters $[2^m, s_m(r), 2^{m-r}]_q$.

Then a parity check matrix of C_{X_r} is given by

$$H_{X_r} = \begin{bmatrix} \gamma_0(\mathbf{x}_{t_m}^1) & \gamma_1(\mathbf{x}_{t_m}^1) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_m}^1) \\ \gamma_0(\mathbf{x}_{t_{m-1}}^1) & \gamma_1(\mathbf{x}_{t_{m-1}}^1) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{m-1}}^1) \\ \gamma_0(\mathbf{x}_{t_{m-1}}^2) & \gamma_1(\mathbf{x}_{t_{m-1}}^2) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{m-1}}^2) \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_0(\mathbf{x}_{t_{m-1}}^{C_{m,m-1}}) & \gamma_1(\mathbf{x}_{t_{m-1}}^{C_{m,m-1}}) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{m-1}}^{C_{m,m-1}}) \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_0(\mathbf{x}_{t_{r+1}}^1) & \gamma_1(\mathbf{x}_{t_{r+1}}^1) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{r+1}}^1) \\ \gamma_0(\mathbf{x}_{t_{r+1}}^2) & \gamma_1(\mathbf{x}_{t_{r+1}}^2) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{r+1}}^2) \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_0(\mathbf{x}_{t_{r+1}}^{C_{m,r+1}}) & \gamma_1(\mathbf{x}_{t_{r+1}}^{C_{m,r+1}}) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{r+1}}^{C_{m,r+1}}) \end{bmatrix},$$

where the elements $\mathbf{x}_{t_{r+j}}^1, \mathbf{x}_{t_{r+j}}^2, \dots, \mathbf{x}_{t_{r+j}}^{C_{m,r+j}}, j = 1, \dots, m-r$, are the $C_{m,r+j} = \binom{m}{r+j}$ elements in \mathbb{Z}_2^m having Hamming weight $r+j$.

For a positive integer u with $r < u < m$, consider the set $X_u = \{\mathbf{x} \in \mathbb{Z}_2^m | wt_H(\mathbf{x}) > u\}$. Let $C_q(u, m) = C_{X_u}$ be the character code with parameters $[2^m, s_m(u), 2^{m-u}]_q$. A parity check matrix for C_{X_u} is given by

$$H_{X_u} = \begin{bmatrix} \gamma_0(\mathbf{x}_{t_m}^1) & \gamma_1(\mathbf{x}_{t_m}^1) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_m}^1) \\ \gamma_0(\mathbf{x}_{t_{m-1}}^1) & \gamma_1(\mathbf{x}_{t_{m-1}}^1) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{m-1}}^1) \\ \gamma_0(\mathbf{x}_{t_{m-1}}^2) & \gamma_1(\mathbf{x}_{t_{m-1}}^2) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{m-1}}^2) \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_0(\mathbf{x}_{t_{m-1}}^{C_{m,m-1}}) & \gamma_1(\mathbf{x}_{t_{m-1}}^{C_{m,m-1}}) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{m-1}}^{C_{m,m-1}}) \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_0(\mathbf{x}_{t_{u+1}}^1) & \gamma_1(\mathbf{x}_{t_{u+1}}^1) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{u+1}}^1) \\ \gamma_0(\mathbf{x}_{t_{u+1}}^2) & \gamma_1(\mathbf{x}_{t_{u+1}}^2) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{u+1}}^2) \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_0(\mathbf{x}_{t_{u+1}}^{C_{m,u+1}}) & \gamma_1(\mathbf{x}_{t_{u+1}}^{C_{m,u+1}}) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{u+1}}^{C_{m,u+1}}) \end{bmatrix},$$

where the elements $\mathbf{x}_{t_{u+j}}^1, \mathbf{x}_{t_{u+j}}^2, \dots, \mathbf{x}_{t_{u+j}}^{C_{m,u+j}}, j = 1, \dots, m-u$, are the $C_{m,u+j} = \binom{m}{u+j}$ elements in \mathbb{Z}_2^m having Hamming weight $u+j$.

Since $u > r$, the parity check matrix H_{X_u} is a submatrix of H_{X_r} and, consequently, we can split H_{X_r} into disjoint submatrices H_{X_u} and H as follows:

$$H_{X_r} = \begin{bmatrix} H_{X_u} \\ \text{---} \\ H \end{bmatrix} =$$

$$\begin{bmatrix} \gamma_0(\mathbf{x}_{t_m}^1) & \gamma_1(\mathbf{x}_{t_m}^1) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_m}^1) \\ \gamma_0(\mathbf{x}_{t_{m-1}}^1) & \gamma_1(\mathbf{x}_{t_{m-1}}^1) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{m-1}}^1) \\ \gamma_0(\mathbf{x}_{t_{m-1}}^2) & \gamma_1(\mathbf{x}_{t_{m-1}}^2) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{m-1}}^2) \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_0(\mathbf{x}_{t_{m-1}}^{C_{m,m-1}}) & \gamma_1(\mathbf{x}_{t_{m-1}}^{C_{m,m-1}}) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{m-1}}^{C_{m,m-1}}) \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_0(\mathbf{x}_{t_{u+1}}^1) & \gamma_1(\mathbf{x}_{t_{u+1}}^1) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{u+1}}^1) \\ \gamma_0(\mathbf{x}_{t_{u+1}}^2) & \gamma_1(\mathbf{x}_{t_{u+1}}^2) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{u+1}}^2) \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_0(\mathbf{x}_{t_{u+1}}^{C_{m,u+1}}) & \gamma_1(\mathbf{x}_{t_{u+1}}^{C_{m,u+1}}) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{u+1}}^{C_{m,u+1}}) \\ \text{---} & \text{---} & \text{---} & \text{---} \\ \gamma_0(\mathbf{x}_{t_u}^1) & \gamma_1(\mathbf{x}_{t_u}^1) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_u}^1) \\ \gamma_0(\mathbf{x}_{t_u}^2) & \gamma_1(\mathbf{x}_{t_u}^2) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_u}^2) \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_0(\mathbf{x}_{t_u}^{C_{m,u}}) & \gamma_1(\mathbf{x}_{t_u}^{C_{m,u}}) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_u}^{C_{m,u}}) \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_0(\mathbf{x}_{t_{r+1}}^1) & \gamma_1(\mathbf{x}_{t_{r+1}}^1) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{r+1}}^1) \\ \gamma_0(\mathbf{x}_{t_{r+1}}^2) & \gamma_1(\mathbf{x}_{t_{r+1}}^2) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{r+1}}^2) \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_0(\mathbf{x}_{t_{r+1}}^{C_{m,r+1}}) & \gamma_1(\mathbf{x}_{t_{r+1}}^{C_{m,r+1}}) & \cdots & \gamma_{n-1}(\mathbf{x}_{t_{r+1}}^{C_{m,r+1}}) \end{bmatrix}.$$

Since $\sum_{i=u+1}^m \binom{m}{i} \geq \sum_{i=r+1}^u \binom{m}{i}$, it follows that $\text{rk} H_{X_u} \geq \text{rk} H$. Then we form the convolutional code V generated by the reduced basic (see Theorem 3.1) generator matrix

$$G(D) = \tilde{H}_{X_u} + \tilde{H}D,$$

where $\tilde{H}_{X_u} = H_{X_u}$ and \tilde{H} is obtained from H by adding zero-rows at the bottom such that \tilde{H} has the number of rows of H_{X_u} in total. By construction, V is a unit memory convolutional code. Since H_{X_u} is the parity check matrix of the code $C_q(u, m) = C_{X_u}$, then H_{X_u} has $2^m - s_m(u)$ linearly independent rows, where $s_m(u) = \sum_{i=0}^u \binom{m}{i}$, hence V has dimension $k_V = 2^m - s_m(u)$. From construction, H has $s_m(u) - s_m(r)$ linearly independent rows and therefore V

has degree $\delta_V = s_m(u) - s_m(r)$. From Theorem 3.1, the free distance d_f of V satisfies $d_f \geq d^\perp$, where d^\perp is the minimum distance of the dual code $[C_q(r, m)]^\perp$. Since the minimum distance of $[C_q(r, m)]^\perp$ is equal to 2^{r+1} , then $d_f \geq 2^{r+1}$. Therefore one can get an $(2^m, 2^m - s_m(u), s_m(u) - s_m(r); 1, d_f \geq 2^{r+1})_q$ convolutional code. \square

Corollary 4.2 *Let \mathbb{F}_q be a finite field of odd characteristic and consider the commutative group $G = (\mathbb{Z}_2^m, +)$ where $m \geq 3$ is an integer. Assume that r and u are positive integers such that the inequalities $r < u < m$ and $\sum_{i=u+1}^m \binom{m}{i} \geq \sum_{i=r+1}^u \binom{m}{i}$ hold. Then there exists an $(2^m, s_m(u), s_m(u) - s_m(r); \mu, d_f \geq 2^{m-u} + 1)_q$ convolutional code where, $s_m(u)$ and $s_m(r)$ are given above.*

Proof: Assume the same notation utilized in the proof of Theorem 4.1. We know that the convolutional code V generated by the generator matrix $G(D) = \tilde{H}_{X_u} + \tilde{H}D$ has parameters $(2^m, 2^m - s_m(u), s_m(u) - s_m(r); 1, d_f \geq 2^{r+1})_q$.

Consider the dual V^\perp of the code V . We know that V^\perp has length $n = 2^m$, dimension $k_{V^\perp} = s_m(u)$ and degree $\delta = s_m(u) - s_m(r)$. We need to compute the free distance d_f^\perp of V^\perp . From Theorem 3.1, one has $\min\{d_0 + d_1, d\} \leq d_f^\perp \leq d$, where d_0 is the minimum distance of the code with parity check matrix H_{X_u} , d_1 is the minimum distance of the code with parity check matrix H and d is the minimum distance of the code with parity check matrix H_{X_r} . We know that $d_0 = 2^{m-u}$ and $d = 2^{m-r}$. Since the minimum distance d_1 is not known we have $d_f^\perp \geq 2^{m-u} + 1$.

Therefore there exists an $(2^m, s_m(u), s_m(u) - s_m(r); \mu, d_f \geq 2^{m-u} + 1)_q$ convolutional code. \square

Example 4.1 *Consider that $m = 5$, $u = 2$ and $r = 1$ and $q = 3$. Thus the inequality $\sum_{i=3}^5 \binom{5}{i} = 16 > \sum_{i=2}^2 \binom{5}{i} = 10$ hold. From Theorem 4.1, there exists an $(32, 17, 10; 1, d_f \geq 4)_3$ convolutional code. Moreover, from Corollary 4.2, there exists an $(32, 15, 10; \mu, d_f \geq 9)_3$ convolutional code. On the other hand, if we take $m = 6$, $u = 2$, $r = 1$ and $q = 3$, one can get $(64, 42, 15; 1, d_f \geq 4)_3$ $(64, 22, 15; \mu, d_f \geq 17)_3$ convolutional codes.*

Next we describe how to construct multi memory convolutional codes derived from character codes.

Theorem 4.3 *Let \mathbb{F}_q be a finite field of odd characteristic and consider the commutative group $G = (\mathbb{Z}_2^m, +)$ where $m \geq 4$ is an integer. Assume that r, u, v are positive integers such that the inequalities $r < v < u < m$, $\sum_{i=u+1}^m \binom{m}{i} \geq$*

$\sum_{i=r+1}^v \binom{m}{i} \geq \sum_{i=v+1}^u \binom{m}{i}$ hold. Then there exist convolutional codes with parameters $(2^m, 2^m - s_m(u), \delta; 2, d_f \geq 2^{r+1})_q$, where $s_m(u)$ is given above and $\delta = \sum_{i=r+1}^v \binom{m}{i}$.

Proof: Adopting the notation of Theorem 4.1, let us consider the parity check matrices H_{X_r} and H_{X_u} of the codes $C_q(r, m)$ and $C_q(u, m)$, respectively, such that

$$H_{X_r} = \begin{bmatrix} H_{X_u} \\ \text{---} \\ H_1 \\ \text{---} \\ H_2 \end{bmatrix},$$

where H_1 and H_2 are submatrices of H_{X_r} with $\sum_{i=v+1}^u \binom{m}{i}$ and $\sum_{i=r+1}^v \binom{m}{i}$ linearly independent rows, respectively. Note that this is possible due to $r < v < u < m$. From hypothesis one has $\text{rk} H_{X_u} \geq \text{rk} H_i$, $i = 1, 2$. Then we form the convolutional code V generated by the matrix

$$G(D) = \tilde{H}_{X_u} + \tilde{H}_1 D + \tilde{H}_2 D^2,$$

where $\tilde{H}_{X_u} = H_{X_u}$. By construction, the code V is a two memory code of dimension $k_V = 2^m - s_m(u)$. Further, the degree of V is equal to $\text{rk} \tilde{H}_2 = \sum_{i=r+1}^v \binom{m}{i}$.

Moreover, from Theorem 3.1, one has $d_f \geq d^\perp$, that is, $d_f \geq 2^{r+1}$. Therefore one can get an $(2^m, 2^m - s_m(u), \delta; 2, d_f \geq 2^{r+1})_q$ convolutional code, where

$$\delta = \sum_{i=r+1}^v \binom{m}{i}. \quad \square$$

Remark 4.4 Note that Theorem 4.1 can be straightforward generalized in order to construct convolutional codes with memory $\mu \geq 3$. We do not present the generalization here since it is trivial.

We now construct convolutional codes derived from group characters codes $C_q(r, m; l)$ and their corresponding dual $[C_q(r, m; l)]^\perp$. To proceed further we utilize the notation $\binom{m}{i}_l$ to denote the cardinality of the set $X_i = \{\mathbf{x} \in \mathbb{Z}_l^m : \|\mathbf{x}\| = i\}$, $0 \leq i \leq m(l-1)$, given by $\binom{m}{i}_l = \sum_{k=0}^m (-1)^k \binom{m}{k} \binom{m-1+i-kl}{m-1}$. Now we are ready to show the next result:

Theorem 4.5 Consider the group $(\mathbb{Z}_l^m, +)$, where $m \geq 3$, $l \geq 3$ are integers, and let F_q be a finite field such that $l|(q-1)$. Assume that r and u are positive integers such that the inequalities $r < u < m(l-1)$ and $\sum_{i=u+1}^m \binom{m}{i}_l \geq \sum_{i=r+1}^u \binom{m}{i}_l$ hold. Then there exists a unit memory convolutional code with parameters $(l^m, l^m - S_m(u), S_m(u) - S_m(r); 1, d_f \geq (b+2)l^a)_q$, where a and b are integers such that $r = a(l-1) + b$, $0 \leq b \leq l-2$ and $S_m(u), S_m(r)$ are given in Section 2.

Proof: Assume that $X(r, m; l) = \{\mathbf{x} \in \mathbb{Z}_l^m : \|\mathbf{x}\| > r\}$ and consider the character code $C_q(r, m; l)$ with parameters $[l^m, S_m(r), (l-b)l^{m-1-a}]_q$, where $0 \leq r < m(l-1)$ is writing as $r = a(l-1) + b$, $0 \leq b \leq l-2$, and $S_m(r) = \sum_{i=0}^r \sum_{k=0}^m (-1)^k \binom{m}{k} \binom{m-1+i-kl}{m-1}$. A parity check matrix for $C_q(r, m; l)$ is given by $H_{X(r, m; l)} = [\gamma_{j-1}(\mathbf{x})]_{\mathbf{x} \in X(r, m; l), 1 \leq j \leq l^m}$. Next, consider the set $X(u, m; l) = \{\mathbf{y} \in \mathbb{Z}_l^m : \|\mathbf{y}\| > u\}$, generating the code $C_q(u, m; l)$ with parity check matrix $H_{X(u, m; l)} = [\gamma_{j-1}(\mathbf{y})]_{\mathbf{y} \in X(u, m; l), 1 \leq j \leq l^m}$.

Since $u > r$, the parity check matrix $H_{X(u, m; l)}$ is a submatrix of $H_{X(r, m; l)}$ and, consequently, we can split the latter matrix into disjoint submatrices $H_{X(u, m; l)}$ and H :

$$H_{X(r, m; l)} = \begin{bmatrix} H_{X(u, m; l)} \\ \hline H \end{bmatrix}.$$

The matrices $H_{X(r, m; l)}$ and $H_{X(u, m; l)}$ have rank $l^m - S_m(r)$ and $l^m - S_m(u)$, respectively, so H has rank $S_m(u) - S_m(r)$. Because $\sum_{i=u+1}^m \binom{m}{i}_l \geq \sum_{i=r+1}^u \binom{m}{i}_l$, one has $\text{rk} H_{X(u, m; l)} \geq \text{rk} H$. Then one obtains the convolutional code V generated by

$$G(D) = \tilde{H}_{X(u, m; l)} + \tilde{H}D.$$

From construction, V is a unit memory convolutional code of length l^m and dimension $l^m - S_m(u)$. Additionally, V has degree $S_m(u) - S_m(r)$. We only need to compute (a lower bound to) d_f . From Theorem 3.1, $d_f \geq d^\perp$, where d^\perp is the minimum distance of $[C_q(r, m; l)]^\perp$. Since the latter code is monomial equivalent to $C_q(m(l-1) - 1 - r, m; l)$, it is easy to verify that $d^\perp = (b+2)l^a$. Therefore, one obtains an $(l^m, l^m - S_m(u), S_m(u) - S_m(r); 1, d_f \geq (b+2)l^a)_q$ convolutional code, as desired. \square

Remark 4.6 Note that Theorem 4.5 can be easily generalized in order to construct multi-memory convolutional codes as well.

5 Code Comparisons

In this section we compare the parameters of the new convolutional codes with the ones displayed in the literature. At the present, it seems that the parameters of the (classical) convolutional codes shown in [12], derived from BCH codes, are the better ones. However, the referred constructions are valid only to primitive BCH codes. Therefore, we compare the new code parameters with the ones exhibited in [1], since the latter paper also brings good convolutional codes. We must note that there exist other good convolutional codes in the literature, but these codes are constructed case-by-case in most situations.

In Table 1, the new code parameters appear in the first column and the parameters of the codes shown in [1] are in the second column. Note that the new code parameters are given by applying Theorem 4.1 and Corollary 4.2.

As can be seen in Table 1, the new codes have parameters better than the ones shown in [1] for almost all cases. Only in two cases the codes available in [1] are better than the new codes.

6 Summary

We have constructed new families of convolutional codes derived from group character codes. These codes are constructed algebraically and not by computational search or even case by case. Moreover, the new code parameters are better than the ones available in the literature.

Acknowledgment

This research has been partially supported by the Brazilian Agencies CAPES and CNPq.

References

- [1] S. A. Aly, M. Grassl, A. Klappenecker, M. Rötteler, P. K. Sarvepalli. Quantum convolutional BCH codes. e-print arXiv:quant-ph/0703113.
- [2] C. Ding, D. Kohel, S. Ling. Elementary 2-group character codes. *IEEE Trans. Inform. Theory*, 46(1):280–284, January 2000.
- [3] G. D. Forney Jr. Convolutional codes I: algebraic structure. *IEEE Trans. Inform. Theory*, 16(6):720–738, November 1970.
- [4] H. Gluesing-Luerssen, J. Rosenthal and R. Smarandache. Strongly MDS convolutional codes. *IEEE Trans. Inform. Theory*, 52:584–598, 2006.
- [5] H. Gluesing-Luerssen, W. Schmale. Distance bounds for convolutional codes and some optimal codes. e-print arXiv:math/0305135.

Table 1: Code Comparisons

The new codes	Codes shown in [1]
$(n, k, \gamma; \mu, d_f)_q$	$(n, k^*, \gamma^*; 1, d_f^*)_q$
$(32, 15, 10; \mu, d_f \geq 9)_3$	$(32, 16, \gamma; 1, d_f \geq 5)_3$
$(64, 42, 15; 1, d_f \geq 4)_3$	$(64, 32, \gamma; 1, d_f \geq 6)_3$
$(64, 22, 15; \mu, d_f \geq 17)_3$	$(64, 16, \gamma; 1, d_f \geq 8)_3$
$(128, 64, 35; 1, d_f \geq 8)_3$	$(128, 64, \gamma; 1, d_f \geq 6)_3$
$(128, 64, 35; 1, d_f \geq 8)_3$	$(128, 32, \gamma; 1, d_f \geq 8)_3$
$(128, 64, 35; \mu, d_f \geq 17)_3$	$(128, 32, \gamma; 1, d_f \geq 8)_3$
$(32, 15, 10; \mu, d_f \geq 9)_5$	$(32, 16, \gamma; 1, d_f \geq 5)_5$
$(64, 42, 15; 1, d_f \geq 4)_5$	$(64, 32, \gamma; 1, d_f \geq 5)_5$
$(64, 22, 15; \mu, d_f \geq 17)_5$	$(64, 16, \gamma; 1, d_f \geq 6)_5$
$(128, 64, 35; 1, d_f \geq 8)_5$	$(128, 64, \gamma; 1, d_f \geq 5)_5$
$(128, 64, 35; 1, d_f \geq 8)_5$	$(128, 32, \gamma; 1, d_f \geq 6)_5$
$(128, 64, 35; \mu, d_f \geq 17)_5$	—
$(32, 15, 10; \mu, d_f \geq 9)_7$	$(32, 16, \gamma; 1, d_f \geq 8)_7$
$(64, 42, 15; 1, d_f \geq 4)_7$	$(64, 48, \gamma; 1, d_f \geq 5)_7$
$(64, 22, 15; \mu, d_f \geq 17)_7$	$(64, 8, \gamma; 1, d_f \geq 14)_7$
$(128, 64, 35; \mu, d_f \geq 17)_7$	$(128, 64, \gamma; 1, d_f \geq 8)_7$
$(128, 64, 35; \mu, d_f \geq 17)_7$	$(128, 16, \gamma; 1, d_f \geq 14)_7$
$(32, 15, 10; \mu, d_f \geq 9)_9$	$(32, 16, \gamma; 1, d_f \geq 8)_9$
$(64, 42, 15; 1, d_f \geq 4)_9$	$(64, 48, \gamma; 1, d_f \geq 5)_9$
$(64, 22, 15; \mu, d_f \geq 17)_9$	$(64, 8, \gamma; 1, d_f \geq 12)_9$
$(128, 64, 35; \mu, d_f \geq 17)_7$	$(128, 64, \gamma; 1, d_f \geq 8)_7$
$(128, 64, 35; \mu, d_f \geq 17)_7$	$(128, 16, \gamma; 1, d_f \geq 12)_7$
$(32, 15, 10; \mu, d_f \geq 9)_{11}$	$(32, 8, \gamma; 1, d_f \geq 6)_{11}$
$(64, 42, 15; 1, d_f \geq 4)_{11}$	$(64, 32, \gamma; 1, d_f \geq 5)_{11}$
$(64, 22, 15; \mu, d_f \geq 17)_{11}$	$(64, 16, \gamma; 1, d_f \geq 6)_{11}$
$(128, 64, 35; 1, d_f \geq 8)_{11}$	$(128, 64, \gamma; 1, d_f \geq 5)_{11}$
$(128, 64, 35; \mu, d_f \geq 17)_{11}$	$(128, 32, \gamma; 1, d_f \geq 6)_{11}$

- [6] H. Gluesing-Luerssen and W. Schmale. On doubly-cyclic convolutional codes. *Applicable Algebra in Eng. Comm. Comput.*, 17(2):151–170, 2006.
- [7] H. Gluesing-Luerssen and F-L Tsang. A matrix ring description for cyclic convolutional codes. *Advances in Math. Communications*, 2(1):55–81, 2008.
- [8] K. J. Hole. On classes of convolutional codes that are not asymptotically catastrophic. *IEEE Trans. Inform. Theory*, 46(2):663–669, March 2000.
- [9] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. University Press, Cambridge, 2003.
- [10] R. Johannesson and K. S. Zigangirov. *Fundamentals of Convolutional Coding*. Digital and Mobile Communication, Wiley-IEEE Press, 1999.
- [11] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inform. Theory*, 52(11):4892–4914, November 2006.
- [12] G. G. La Guardia. On nonbinary quantum convolutional BCH codes. *Quantum Inform. Computation*, 12(9-10):0820–0842, 2012.
- [13] L. N. Lee. Short unit-memory byte-oriented binary convolutional codes having maximum free distance. *IEEE Trans. Inform. Theory*, 22:349–352, May 1976.
- [14] S. Ling. A family of group character codes. *European J. of Combinatorics* 25: 579-590, 2004.
- [15] Ph. Piret. *Convolutional Codes: An Algebraic Approach*. Cambridge, Massachusetts: The MIT Press, 1988.
- [16] Ph. Piret. A convolutional equivalent to Reed-Solomon codes. *Philips J. Res.*, 43:441–458, 1988.
- [17] Ph. Piret and T. Krol. MDS convolutional codes. *IEEE Trans. Inform. Theory*, 29(2):224–232, 1983.
- [18] J. Rosenthal and R. Smarandache. Maximum distance separable convolutional codes. *Applicable Algebra in Eng. Comm. Comput.*, 10:15–32, 1998.
- [19] J. Rosenthal and E. V. York. BCH convolutional codes. *IEEE Trans. Inform. Theory*, 45(6):1833-1844, 1999.
- [20] R. Smarandache, H. G.-Luerssen, J. Rosenthal. Constructions of MDS-convolutional codes. *IEEE Trans. Inform. Theory*, 47(5):2045–2049, July 2001.